Internet Use Policy

Summary: The following is ThomasArt's (TA) internet use policy. These rules are in place to protect both ThomasArts and each employee. Inappropriate use exposes ThomasArts to many risks including virus attacks, compromise of services and legal issues.

Policy

While ThomasArts's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems or accounts remains the property of ThomasArts. Because of the need to protect ThomasArts's resources, management cannot guarantee the confidentiality of information stored on any network device belonging to ThomasArts or third-party accounts.

Employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager. ThomasArts strongly recommends that any information that users consider sensitive or vulnerable be encrypted.

For security and network maintenance purposes, authorized individuals within ThomasArts may monitor equipment, systems, and network traffic at any time. ThomasArts reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Because information contained on portable computers is especially vulnerable, special care should be exercised. No employee shall disable or remove security software that has been installed by the ThomasArts. Employees shall take appropriate steps to physically protect the laptop from theft or unauthorized access.

Industry related postings by employees from a ThomasArts email address that may be seen by the public should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of ThomasArts, unless posting is during business duties. Systems used by the employee that are

connected to the ThomasArts Internet/Intranet/Extranet, whether owned by the employee or ThomasArts, shall use approved anti-malware software.

Employees must use extreme caution when opening email attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code. Employees should also be careful of emails which include links to suspicious Web sites. If you are unsure of an email's authenticity, contact the security group or the helpdesk for assistance.

If you feel a website you are trying to reach is incorrectly being blocked, please submit a support request ticket, and include the URL, the purpose and if this a permanent or temporary request.